

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-303114

(43)Date of publication of application : 24.10.2003

(51)Int.Cl.

G06F 11/00

G06F 1/00

G06F 9/445

G06K 17/00

(21)Application number : 2002-317984

(71)Applicant : C:KK

(22)Date of filing : 31.10.2002

(72)Inventor : HATA ATSUSHI

(30)Priority

Priority number : 2002029168

Priority date : 06.02.2002

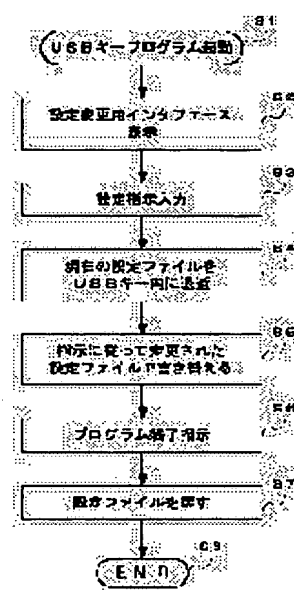
Priority country : JP

(54) SECURITY MAINTENANCE SYSTEM AND USB KEY

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a security maintenance system and a USB key capable of easily changing settings of a browser and a mailer for preventing invasion of a computer virus according to a security level, diagnosing a security hole condition in compliance with a personal computer condition, and easily applying a patch to the security hole.

**SOLUTION:** In this security maintenance system and the USB key, a program inside the USB key changes settings of the browser and the mailer according to a security level and checks a PC condition to output it to a Web server 3. The Web server 3 diagnoses whether the latest patch is applied in compliance with the PC condition or not, displays the diagnosis result to the PC, and urges that the patch should be applied according to guidance if the patch is not applied.



【図2】

## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-303114

(P2003-303114A)

(43)公開日 平成15年10月24日(2003. 10. 24)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

テマコート\*(参考)

G 0 6 F 11/00

G 0 6 K 17/00

L 5 B 0 5 8

1/00

G 0 6 F 9/06

6 6 0 N 5 B 0 7 6

9/445

6 5 0 K

G 0 6 K 17/00

6 3 0 B

6 6 0 Z

審査請求 未請求 請求項の数15 O L (全 11 頁)

(21)出願番号 特願2002-317984(P2002-317984)

(71)出願人 301068930

株式会社シーアイ

東京都豊島区池袋二丁目43番1号 池袋青

柳ビル10F

(22)出願日 平成14年10月31日(2002. 10. 31)

(72)発明者 畑 温

東京都豊島区池袋二丁目43番1号 池袋青

柳ビル10F 株式会社シーアイ内

(31)優先権主張番号 特願2002-29168(P2002-29168)

(32)優先日 平成14年2月6日(2002. 2. 6)

(33)優先権主張国 日本 (J P)

(74)代理人 100093104

弁理士 船津 暢宏 (外1名)

Fターム(参考) 5B058 CA01 CA27 KA02 KA21 KA31

YA13

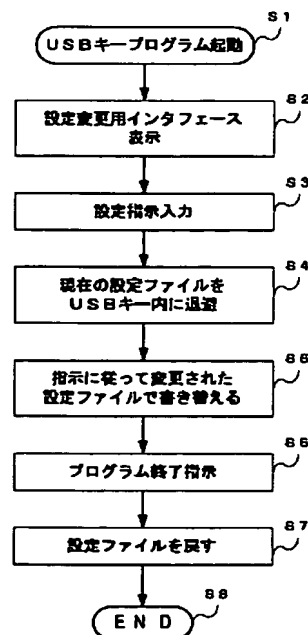
5B076 BA10 BB04 BB18 BB19 EA01

(54)【発明の名称】 セキュリティ保全システム及びUSBキー

(57)【要約】

【課題】 本発明は、コンピュータウィルスの侵入防止のために、ブラウザー及びメーラーの設定をセキュリティのレベルに応じて容易に変更でき、パソコンの状態に応じてセキュリティホールの状況を診断し、そのセキュリティホールに対して容易にパッチを当てることができるセキュリティ保全システム及びUSBキーを提供する。

【解決手段】 USBキー内のプログラムが、ブラウザー及びメーラーの設定をセキュリティのレベルに応じて変更し、またPCの状態をチェックしてWebサーバ3に出力し、Webサーバ3は、当該PC状態に応じて最新のパッチが当てられているか否かを診断してPC向けに表示し、パッチが当てられていなければガイダンスに従ってパッチを当てよう促すセキュリティ保全システム及びUSBキーである。



(2)

## 【特許請求の範囲】

【請求項 1】 コンピュータの USB ポートに接続される USB キーであって、

前記 USB ポートに前記 USB キーが差し込まれた状態で、前記コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、前記 USB キーを前記 USB ポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録することを特徴とする USB キー。

【請求項 2】 変更可能な設定ファイルが、ユーザの指定により設定事項をセキュリティの程度に応じて変更可能であることを特徴とする請求項 1 記載の USB キー。

【請求項 3】 コンピュータの USB ポートに接続される USB キーであって、

前記 USB ポートに前記 USB キーが差し込まれた状態で、コンピュータに搭載された OS の状態をチェックし、当該 OS に関する情報を予め記憶する URL のサイトに接続し、前記情報を前記サイトのウェブサーバに出力するコンピュータプログラムを記憶することを特徴とする USB キー。

【請求項 4】 請求項 3 記載の USB キーから提供された OS に関する情報に対して、当該 OS のセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てするためのガイダンスを表示するウェブサーバを有することを特徴とするセキュリティ保全システム。

【請求項 5】 USB キーがコンピュータの USB ポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、前記コンピュータは前記 USB キー内に記憶する URL にアクセスして OS に関する情報をウェブサーバに提供することを特徴とする請求項 4 記載のセキュリティ保全システム。

【請求項 6】 ウェブサーバは、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示することを特徴とする請求項 4 又は 5 記載のセキュリティ保全システム。

【請求項 7】 コンピュータの USB ポートに接続される USB キーであって、

前記 USB ポートに前記 USB キーが差し込まれた状態で、前記コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該 USB キー内に記憶する URL にアクセスして当該コンピュータの OS に関する情報及びコピーした設定ファイルをウェブサーバに提供し、前記 OS に関する情報と前記コピーした設定ファイルから前記ウェブサーバが用意したセキュリティに関する設定ファイルを前記コンピュータで使用可能とするコンピュー

2

タプログラムを記録することを特徴とする USB キー。

【請求項 8】 請求項 7 記載の USB キーから提供された OS に関する情報及びコピーした設定ファイルに対して、当該 OS に関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有することを特徴とするセキュリティ保全システム。

【請求項 9】 USB キーがコンピュータの USB ポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、前記コンピュータは前記 USB キー内に記憶する URL にアクセスして OS に関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供することを特徴とする請求項 8 記載のセキュリティ保全システム。

【請求項 10】 変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されていることを特徴とする請求項 1 又は 2 記載の USB キー。

【請求項 11】 新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていなければ当該プロセスを動作させないプロセス監視機能を備えたことを特徴とする請求項 1 又は 2、若しくは請求項 10 のいずれか記載の USB キー。

【請求項 12】 OS に関する情報の問い合わせに対して OS に関する情報の出力を停止するロック機能を備えたことを特徴とする請求項 11 記載の USB キー。

【請求項 13】 特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えたことを特徴とする請求項 11 又は 12 記載の USB キー。

【請求項 14】 コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えたことを特徴とする請求項 1 又は 2、若しくは請求項 11 乃至 13 のいずれか記載の USB キー。

【請求項 15】 コンピュータのメモリ常駐を不許可とした上で、ファイル内容をテキストに変換してコンピュータで表示させる機能を備えたことを特徴とする請求項 14 記載の USB キー。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、USB (Universal Serial Bus) キーを用いたセキュリティ保全システムに係り、特に、ブラウザ及びメーラーの設定を簡易に変更することでコンピュータウィルスの侵入を防止する

(3)

3

と共に、パソコンのOS (Operating System) におけるセキュリティホールにパッチを当てることを手助けするセキュリティ保全システム及びUSBキーに関する。

【0002】

【従来の技術】インターネットにアクセスした際に、パーソナルコンピュータ (パソコン: PC) のセキュリティホールを狙って、コンピュータウィルスが侵入することがある。このため、OS提供会社は、コンピュータウィルスの侵入を防ぐために、そのセキュリティホールにパッチを当てるための情報及びパッチ用プログラムを提供している。

【0003】

【発明が解決しようとする課題】しかしながら、OS提供会社の提供する情報に従ったブラウザ及びメーラーの設定変更は、パソコン初心者には難しく、設定変更をうまく行うことができないという問題点があった。また、セキュリティホールにパッチを当てるプログラムは提供されているものの、実際のパッチを当てる作業はパソコン初心者には難しく、容易にパッチを当てることができないという問題点があった。更に、PCユーザは、定期的にOS提供会社の情報にアクセスして自機を最新のセキュリティ保全状態としなければならず、メンテナンスが面倒であるとの問題点があった。

【0004】本発明は上記実情に鑑みて為されたもので、コンピュータウィルスの侵入を防ぐために、パソコン初心者でもブラウザ及びメーラーの設定をセキュリティのレベルに応じて容易に変更できるUSBキーを提供することを目的とする。

【0005】また、本発明の別の目的は、パソコンの状態に応じてセキュリティホールの状況を診断し、そのセキュリティホールに対してパソコン初心者でも容易にパッチを当てることのできるセキュリティ保全システム及びUSBキーを提供することにある。

【0006】

【課題を解決するための手段】上記従来例の問題点を解決するための本発明は、コンピュータのUSBポートに接続されるUSBキーにおいて、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、USBキーをUSBポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録するものであり、当該USBキーでブラウザ、メーラーの設定ファイルを容易にセキュリティを向上させるための設定ファイルに変更でき、更にUSBキーを抜き出す際には、設定を簡単に元に戻すことができる。

【0007】本発明は、上記USBキーにおいて、変更可能な設定ファイルが、ユーザの指定により設定事項を

4

セキュリティの程度に応じて変更可能としたものであり、セキュリティの程度によって細かく設定事項をユーザが指定できる。

【0008】本発明は、コンピュータのUSBポートに接続されるUSBキーにおいて、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されたOSの状態をチェックし、当該OSに関する情報を予め記憶するURLのサイトに接続し、その情報を当該サイトのウェブサーバに出力するコンピュータプログラムを記憶するものであり、USBキーが挿入されたコンピュータのOSの状態をウェブサーバに容易に提供できる。

【0009】本発明は、セキュリティ保全システムにおいて、上記USBキーから提供されたOSに関する情報に対して、ウェブサーバが、当該OSのセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てるためのガイダンスを表示するものであり、ウェブサーバによるコンピュータのOSの状態を診断することで、ユーザはコンピュータの安全性を容易に認識でき、コンピュータを常に最新のセキュリティ状態としておくことができる。

【0010】本発明は、上記セキュリティ保全システムにおいて、USBキーがコンピュータのUSBポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはUSBキー内のURLにアクセスしてOSに関する情報をウェブサーバに提供するものであり、コンピュータの電源オン時には必ずOSの状態が診断され、コンピュータのセキュリティを向上させることができる。

【0011】本発明は、上記セキュリティ保全システムにおいて、ウェブサーバが、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示するものであり、ユーザはコンピュータの安全性を容易に認識できるだけでなく、セキュリティに関連する情報もウェブサイトから得ることができる。

【0012】本発明は、コンピュータのUSBポートに接続されるUSBキーであって、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該USBキー内に記憶するURLにアクセスして当該コンピュータのOSに関する情報及びコピーした設定ファイルをウェブサーバに提供し、OSに関する情報とコピーした設定ファイルからウェブサーバが用意したセキュリティに関する設定ファイルをコンピュータで使用可能とするコンピュータプログラムを記録するものであり、コンピュータのOSの状態とセキュリティの設定ファイルの内容から適正な設定ファイルをウェブサーバより取得できる。

(4)

5

【0013】本発明は、セキュリティ保全システムにおいて、請求項7記載のUSBキーから提供されたOSに関する情報及びコピーした設定ファイルに対して、当該OSに関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有するものであり、コンピュータにおけるセキュリティをチェックしてセキュリティを確保できる。

【0014】本発明は、上記セキュリティ保全システムにおいて、USBキーがコンピュータのUSBポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはUSBキー内に記憶するURLにアクセスしてOSに関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供するものであり、コンピュータの電源オン時には必ずOSの状態及びセキュリティに関する設定ファイルの内容が診断され、コンピュータのセキュリティを向上させることができる。

【0015】本発明は、上記USBキーにおいて、変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されているものであり、コンピュータウィルス感染を防止できる。

【0016】本発明は、上記USBキーにおいて、新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていない場合は当該プロセスを動作させないプロセス監視機能を備えたものであり、コンピュータウィルス感染を防止できる。

【0017】本発明は、上記USBキーにおいて、OSに関する情報の問い合わせに対してOSに関する情報の出力を停止するロック機能を備えたものであり、コンピュータウィルスの侵入を防止できる。

【0018】本発明は、上記USBキーにおいて、特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えたものであり、コンピュータウィルス感染が予想されるファイルをチェックでき、感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることで、コンピュータを保全できる。

【0019】本発明は、上記USBキーにおいて、コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えたものであり、コンピュータウィルス感染を防止できる。

【0020】本発明は、上記USBキーにおいて、コンピュータのメモリ常駐を不許可とした上で、ファイル内容をテキストに変換してコンピュータで表示させる機能

6

を備えたものであり、コンピュータウィルスに感染したファイルの内容をテキストで確認できる。

【0021】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るUSBキーは、パソコン(PC)に搭載されたブラウザ及びメーラーの設定を、コンピュータウィルスの侵入を防止するよう変更するプログラムを記憶しており、USBポートにそのUSBキーが差し込まれている時は、そのプログラムに従ってPCが動作してブラウザ等の設定を変更し、USBキーを抜き出す際には、変更前の設定に戻すものであり、USBキー挿入時に設定変更を容易に行い、セキュリティを向上させることができるものである。

【0022】また、本発明の実施の形態に係るUSBキーを用いたセキュリティ保全システムは、USBキー内のプログラムがPCの状態をチェックしてWebサーバ3に出力し、Webサーバ3は、当該PC状態に応じて最新のパッチが当てられているか否かを診断してPC向けに表示し、パッチが当てられていなければガイダンスに従ってパッチを当てるよう促すようにしているので、ユーザはPCの最新状況を知ることができ安心であり、また、ガイダンスに従うと容易にパッチを当てることができるものである。

【0023】本発明の実施の形態に係るセキュリティ保全システムの構成について図1を参照しながら説明する。図1は、本発明の実施の形態に係るセキュリティ保全システムの構成ブロック図である。本発明の実施の形態に係るセキュリティ保全システム(本システム)は、図1に示すように、USBキー1と、パソコン(PC)2と、ウェブ(Web)サーバ3とを有している。USBキー1は、PC2のUSBポートに挿入されるものである。PC2は、インターネットを介してWebサーバ3に接続可能となっている。

【0024】本システムにおける各部を具体的に説明する。USBキー1は、以下に説明するプログラムとデータを記憶している。USBキー1に記憶されているプログラムは、(1)ブラウザ及びメーラーの設定変更を行うためのプログラム、(2)Webサーバ3にアクセスするための制御を行うプログラム、(3)自PCの状態をチェックし、その情報をWebサーバ3に出力するプログラムである。また、USBキー1に記憶されているデータは、(1)ブラウザ及びメーラーの設定ファイル、(2)WebサーバにアクセスするためのURL(UniformResource Locator)であり、また、設定変更前の元の設定ファイルが一時的に記憶される。

【0025】PC2は、USBキー1内のプログラムを動作させるコンピュータで、ブラウザ及びメーラーの設定ファイルを変更し、また、自機のOS状態をチェックして、その状態に関するデータを、インターネットを

(5)

7

介してWebサーバ3にアクセスして出力する。

【0026】Webサーバ3は、OS提供会社のセキュリティホールに関する情報、コンピュータウイルス及びワクチンソフトに関する情報を提供する。また、Webサーバ3は、PC2からそのOSの状態に関するデータを受け取ると、そのOSが最新のセキュリティ状態となっているか否かを判断（診断）し、OS提供会社からパッチ用プログラムが提供されているにも拘わらず、そのOSにはパッチ用プログラムが当てられていない（最新のセキュリティ状態ではない）ものであると、パッチ用プログラムでパッチを当てる操作をWeb上でガイダンス表示する。

【0027】従って、Webサーバ3は、PC2のOSの種類に応じて診断を行い、またOSの状態に応じたガイダンス表示を行う。PC2のユーザは、当該ガイダンスに従ってパッチ用プログラムをPC2にダウンロードしてパッチを当てるようにすれば、初心者でも容易にその作業を行うことができる。

【0028】次に、本システムの動作について図2～図4を参照しながら説明する。図2は、ブラウザー及びメーラーの設定変更の処理を示すフロー図であり、図3は、OS状態をチェックして提供する処理を示すフロー図であり、図4は、Webサーバ3における処理を示すフロー図である。

【0029】図2に示すように、USBキー1内のブラウザー及びメーラーの設定ファイルを変更するプログラムは、PC2内で起動し（S1）、設定変更用のインターフェースを表示する（S2）。次に、PC2のユーザによって設定指示の入力が行われ（S3）、現在の設定ファイルをUSBキー1内に退避する（S4）。

【0030】次に、処理S3における指示に従って変更された設定ファイルで書き替える（S5）。書き替えは、予めUSBキー1内に変更用の設定ファイルが記憶されており、処理S3によってユーザがセキュリティの程度に応じて設定事項を指定して変更用の設定ファイルを作成し、その変更用の設定ファイルとブラウザー等に既に記憶されている設定ファイルとを置き換えるというものである。

【0031】そして、PC2からプログラム終了の指示が入力されると（S6）、処理S4でUSBキー1内に退避した元の設定ファイルに戻す処理を行う（S7）。そして、プログラムが終了する（S8）。このようにして、PC2内のブラウザー及びメーラーの設定ファイルの変更を初心者でも容易に行うことができる。

【0032】次に、図3を用いてPC2のOS状態チェック及びそのデータの提供について説明する。図3に示すように、USBキー1内のOS状態チェック及びデータ提供のプログラムが起動されると（S11）、OSの状態をチェックする（S12）。OS状態チェックは、当該プログラムがOSの種類、バージョンアップされた

8

ファイル等を参照し、PC2の現在のOSに関するデータ（PC状態情報）を取得し、USBキー1内に一時的に記憶する。

【0033】そして、PC2は、USBキー1内に記憶しているURLにインターネット経由でアクセスし（S13）、Webサーバ3に一時的に記憶したPC状態情報を提供する（S14）。これで、PC2側の処理を終了する（S15）。ここで、Webサーバ3へのアクセスは、PC2にUSBキー1が挿入された状態で、PC2の電源がオンになると、自動的に行うようにしてもよいし、PC2でUSBキー1内のプログラムを起動して手動にて行うようにしてもよい。

【0034】次に、PC2からPC状態情報を入力したWebサーバ3の処理について図4を用いて説明する。図4に示すように、PC2からPC状態情報を入力したWebサーバ3は処理を開始し（S21）、PC状態情報に示されたPC状態（当該PCのOSの状態）に応じた情報を参照する（S22）。具体的には、提供されるPC状態情報からOSの種類、バージョンアップ状況を認識し、当該PCにおける現在のOSに関するセキュリティホール及びパッチに関する情報を参照する。

【0035】そして、PC状態情報からPC2におけるOSの全てのセキュリティホールにパッチが当てられているか否かを判断（診断）し（S23）、パッチが当てられていなければ（Noの場合）、パッチが当てられていないセキュリティホールにパッチを当てるガイダンスを出力し（S24）、そのガイダンスに従ってユーザにはパッチ当てを行わせる。また、パッチが当てられていれば（Yesの場合）、パッチが当てられている旨をPC2向けに表示する（S25）。

【0036】このように、PC2は、USBキー1が差し込まれている状態であれば、Webサーバ3にアクセスして当該PCの状態を報告し、Webサーバ3では、報告（提供）されたPC状態から現在の状況が最新の状態にてパッチが当てられているか否かを知らせることができ、パッチが当てられていなければ、操作ガイダンスに従ってパッチを当てる作業を容易に行うことができる。つまり、ユーザは、PC2のOSに対して安全性を容易に認識できるものである。

【0037】尚、Webサーバ3にアクセスした時には、PC2の状態の診断結果を表示するだけでなく、関連するコンピュータウイルス及びワクチンソフトウェアの最新情報も表示すると、PCユーザにとってネットワークのセキュリティ関連の最新情報を知ることができて便利である。

【0038】また、本発明の別の実施の形態に係るセキュリティ保全システム（別のシステム）について説明する。この別のシステムは、構成としては図1のものと同様であるが、USBキー1内のプログラムの動作が本システムのものとは異なっている。別のシステムは、USB

(6)

9

キー1がPC2に挿入された状態で、USBキー1内のプログラムを動作させると、そのプログラムがUSBキー1内に記述されたURL及びUSBキー1の装置IDを読み込み、更にPC2におけるOSに関する情報とセキュリティに関する設定ファイルのコピーを読み込み、上記URLの示すサイトにアクセスしてUSBキーの装置ID、OSに関する情報及び設定ファイルのコピーを送信する。

【0039】サイトを管理するサーバ3は、PC2から受信したUSBキー1の装置IDから登録されたユーザを特定し、サーバ3で管理するユーザのOSに関する情報と受信したOSに関する情報とを比較し、OSの状態に変化があったか否かをチェックする。

【0040】また、サーバ3は、受信した設定ファイルのコピーを参照し、OSの状態の関係からセキュリティ上で問題のない設定ファイルであるか否かチェックする。セキュリティ上問題があれば、適正な設定ファイルをPC2にダウンロード可能とする。若しくは、適正な設定ファイルの内容となるようサイト上でガイダンス表示を行い、ユーザ自身に設定ファイルの内容を変更させることもできる。

【0041】別のシステムにおけるUSBキー1内に記憶された起動プログラムについて図5を参照しながら説明する。図5は、本発明の実施の形態に係る別のセキュリティ保全システムのUSBキー内における起動プログラムの処理の流れを示すフローチャートである。別のシステムにおけるUSBキー1に記憶された起動プログラムは、図5に示すように、起動される(S31)と、USBキー1内に記憶されたURL、USBキー1内の装置IDを読み込み(S32)、更にPC2のハードディスクにアクセスしてOSに関する情報を取得し(S33)、セキュリティの設定ファイルをコピーする(S34)。

【0042】次に、プログラムは、読み込んだURLでサーバ3へのアクセスを行い(S35)、サーバ3へ装置のID、OSに関する情報、それにコピーした設定ファイルを提供する(S36)。

【0043】そして、プログラムは、サーバ3から提供された設定ファイルをダウンロードして(S37)、USBキー1内に記憶する。このようにして、サーバ3に対する処理を終了する(S38)。

【0044】そして、プログラムは、PC2内に設定されているセキュリティの設定ファイルを退避し、そのダウンロードした設定ファイルを用いてインターネットへのアクセス、またメールの送受信を行う。

【0045】これに対して、サーバ3での処理について図6を参照しながら説明する。図6は、本発明の別の実施の形態に係るセキュリティ保全システムにおけるサーバ3での処理の流れを示すフローチャートである。サーバ3は、図6に示すように、PC2からアクセスされ

10

(S41)、装置ID、OSに関する情報、セキュリティの設定ファイルのコピーを受信する(S42)と、当該装置IDからユーザを特定し(S43)、サーバ3で管理するユーザのOSに関する情報と受信したOSに関する情報を比較し(S44)、一致するか否かの判定を行う(S45)。

【0046】OSのバージョンアップが為されていれば、不一致が生じるので、不一致の場合(Noの場合)、サーバ3で管理しているユーザのOSに関する情報を受信したOSに関する情報で更新する(S46)。尚、一致する場合(Yesの場合)、情報の更新は行わない。

【0047】次に、不一致の場合に更新されたOSに関する情報、若しくは一致の場合は更新されないOSに関する情報に基づいて、サーバ3はセキュリティの設定ファイルの内容を参照し、当該OSに対する十分なセキュリティが確保されているか判断する(S47)。その設定ファイルでセキュリティが確保されていれば(Yesの場合)、ユーザのPC2の画面に十分なセキュリティであり、ダウンロード不要の旨を表示させる(S48)。十分なセキュリティが確保されていなければ(Noの場合)、セキュリティが確保された安全な設定ファイルをユーザのPC2にダウンロード可能に提供する(S49)。そして、処理を終了する。

【0048】上記別のシステムでは、PC2で現在使用されているセキュリティの設定ファイルをそのOSに関する情報との関連でセキュリティが確保されているか否かをサーバ3が判断しているので、USBキー1を装着したPC2では、現在の利用状況に対するセキュリティを確保でき、新たに登場するOSのセキュリティホールを突いた攻撃に対応できる。

【0049】尚、上記別のシステムでは、USBキー1内のプログラムをユーザが動作させることでセキュリティの確保を実現しているが、PC2にUSBキー1が挿入された状態でPC2が電源オンとなった時に、オートラン機能を用いて自動的に当該プログラムを起動するようにしてもよい。これにより、PC2の電源投入(オン)時に、PC2のOSの状態及び設定ファイルの内容を診断でき、セキュリティ確保された設定ファイルをPC2に提供可能となるものである。

【0050】また、OSに関する情報との関係で、サーバ3に提供したコピーのセキュリティに関する設定ファイルでは十分なセキュリティを確保できない場合に、安全な設定ファイルに置き換えられるようダウンロード可能としているが、サーバ3のサイトの画面上で、ユーザがセキュリティ関連の項目を選択しながらセキュリティの設定ファイルを作成するようにしてもよい。

【0051】尚、上記処理では、プログラムがサーバ3にセキュリティの設定ファイルのコピーを送信するようにしているが、コピーを送信せず、OSに関する情報だ



(7)

11

けで、対応するセキュリティの設定ファイルをダウンロード可能としてもよい。

#### 【0052】

【実施例】次に、本発明の実施の形態に係るUSBキーの一実施例を説明する。USBキー1には、PC2のUSBポートに差し込んだ際に、セキュリティ設定に関するプログラムが自動的に起動するようプログラム化されている。自動起動によって図7に示す画面が表示される。図7は、本発明の実施の形態に係るセキュリティ設定の画面の概略図である。

【0053】図7に示すように、セキュリティ設定の画面は、複数のセキュリティに関する「チェックボックス」「セキュリティの選択バー」、それに「tmp read」「拡張機能」「終了」のボタンが表示される。チェックボックスの「マクロ」は、オフィスソフトの機能を制限し、マクロ型ウィルスの感染を防止するためのものであり、「スクリプト」は、Java（登録商標）スクリプトとVBスクリプトの動作を制限するためのものであり、「JAVA（登録商標）」は、その機能を停止するためのものであり、「cookie（登録商標）」は、その全ての機能を停止するためのものであり、「memory」は、不正メモリアクセスを禁止するためのものである。

【0054】また、「セキュリティの選択バー」は、バーを「高」又は「低」方向に動かすことで、チェックボックスの設定を自動的に行うものである。例えば、選択バーが「低」であれば、チェックボックスの全てを制限しないよう設定し、選択バーを「高」に動かすことで、「マクロ」「スクリプト」の順に機能制限を設定し、選択バーが「高」でチェックボックスの全てを制限する設定にするものである。

【0055】セキュリティ設定の規定値は、選択バーが「高」の位置、すなわち、チェックボックスの全ての機能が制限された状態としている。これにより、ウィルス対策が万全となるものである。

【0056】また、セキュリティ設定画面における「tmp read」とは、ウィルスに感染していると思われるファイルの内容をテキストに変換して表示する機能である。この機能を実行する際には、（1）システム領域への不正アクセスを禁止し、（2）新規ファイルの自動作成を禁止し、（3）ハードディスク（HDD）等の記憶装置内のファイルへの不正アクセスを禁止して、メモリ常駐を不許可とした上で、対象ファイルの内容をテキストとして表示するものである。

【0057】上記（1）～（3）の禁止機能は、本実施例のUSBキー1の基本機能であり、USBキー1をPC2のUSBポートに差し込んだ時に、それら機能が動作するようになっている。この3つの禁止機能によって、ウィルス感染を防止している。

【0058】次に、USBキー1の別の機能を説明する。USBキー1のセキュリティ関連のプログラムに

12

は、プロセス監視機能を備えている。プロセス監視機能とは、正規にレジストリに登録されたプログラムをチェックし、新規プロセスが発生すると、レジストリ内をサーチし、正規プロセスか否かを判定し、正規プロセスでなければ、そのプロセスを動作させないようにしたものである。これにより、正規でないプロセスの動作を停止でき、ウィルス感染を防止できる。

【0059】また、USBキー1のセキュリティ関連のプログラムには、ロック機能を備えている。ロック機能とは、ウィルスが侵入してくる際に、PC2のOSのバージョン情報を問い合わせることがあるが、その問い合わせにOS情報を提供しないようにロックするものである。これにより、ウィルス侵入を防止できる。

【0060】また、USBキー1のセキュリティ関連のプログラムには、メールに添付されたファイルやユーザが指定したファイルのウィルス感染をインターネットの特定サイトにアクセスしてチェックを行い、そのファイルをオンラインバックアップする機能を備えている。この機能は、図7における「拡張機能」に含まれるものである。これにより、ウィルス感染の予想されるファイルをチェックでき、感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることができ、PC2を安全に保つことができる。

【0061】また、「拡張機能」の一つとして、オンラインウィルス駆除の機能がある。この機能を選択すると、特定サイトにオンラインアクセスし、PC2のウィルス駆除を行い、レポートを提供するものである。

【0062】また、USBキー1のセキュリティ関連のプログラムには、最新のシステムとワクチンに関する情報を提供するサイトにアクセス可能となっており、そのサイトのガイダンスに従うと簡単な操作でシステムとワクチンの更新ができるようになっている。

#### 【0063】

【発明の効果】本発明によれば、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、USBキーをUSBポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録するUSBキーとしているので、当該USBキーでブラウザ、メーラーの設定ファイルを容易にセキュリティを向上させるための設定ファイルに変更でき、更にUSBキーを抜き出す際には、設定を簡単に元に戻すことができる効果がある。

【0064】本発明によれば、変更可能な設定ファイルが、ユーザの指定により設定事項をセキュリティの程度に応じて変更可能とした上記USBキーとしているので、セキュリティの程度によって細かく設定事項をユーザが指定できる効果がある。

(8)

13

【0065】本発明によれば、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されたOSの状態をチェックし、当該OSに関する情報を予め記憶するURLのサイトに接続し、その情報を当該サイトのウェブサーバに出力するコンピュータプログラムを記憶するUSBキーとしているので、USBキーが挿入されたコンピュータのOSの状態をウェブサーバに容易に提供できる効果がある。

【0066】本発明によれば、上記USBキーから提供されたOSに関する情報に対して、ウェブサーバが、当該OSのセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てるためのガイダンスを表示するセキュリティ保全システムとしているので、ウェブサーバによるコンピュータのOSの状態を診断することで、ユーザはコンピュータの安全性を容易に認識でき、コンピュータを常に最新のセキュリティ状態としておくことができる効果がある。

【0067】本発明によれば、USBキーがコンピュータのUSBポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはUSBキー内のURLにアクセスしてOSに関する情報をウェブサーバに提供する上記セキュリティ保全システムとしているので、コンピュータの電源オン時には必ずOSの状態が診断され、コンピュータのセキュリティを向上させることができる効果がある。

【0068】本発明によれば、ウェブサーバが、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示する上記セキュリティ保全システムとしているので、ユーザはコンピュータの安全性を容易に認識できるだけでなく、セキュリティに関連する情報もウェブサイトから得ることができる効果がある。

【0069】本発明によれば、コンピュータのUSBポートに接続されるUSBキーであって、USBポートにUSBキーが差し込まれた状態で、コンピュータに搭載されているブラウザ又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該USBキー内に記憶するURLにアクセスして当該コンピュータのOSに関する情報及びコピーした設定ファイルをウェブサーバに提供し、OSに関する情報とコピーした設定ファイルからウェブサーバが用意したセキュリティに関する設定ファイルをコンピュータで使用可能とするコンピュータプログラムを記録するものであり、コンピュータのOSの状態とセキュリティの設定ファイルの内容から適正な設定ファイルをウェブサーバより取得できる効果がある。

【0070】本発明によれば、請求項7記載のUSBキーから提供されたOSに関する情報及びコピーした設定

14

ファイルに対して、当該OSに関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有するセキュリティ保全システムとしているので、コンピュータにおけるセキュリティをチェックしてセキュリティを確保できる効果がある。

【0071】本発明によれば、USBキーがコンピュータのUSBポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはUSBキー内に記憶するURLにアクセスしてOSに関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供する上記セキュリティ保全システムとしているので、コンピュータの電源オン時には必ずOSの状態及びセキュリティに関する設定ファイルの内容が診断され、コンピュータのセキュリティを向上させることができる効果がある。

【0072】本発明によれば、変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されている上記USBキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【0073】本発明によれば、新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていなければ当該プロセスを動作させないプロセス監視機能を備えた上記USBキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【0074】本発明によれば、OSに関する情報の問い合わせに対してOSに関する情報の出力を停止するロック機能を備えた上記USBキーとしているので、コンピュータウィルスの侵入を防止できる効果がある。

【0075】本発明によれば、特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えた上記USBキーとしているので、ウィルス感染が予想されるファイルをチェックでき、コンピュータウィルス感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることで、コンピュータを保全できる効果がある。

【0076】本発明によれば、コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えた上記USBキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【0077】本発明によれば、コンピュータのメモリ常驻を不許可とした上で、ファイル内容をテキストに変換

(9)

15

してコンピュータで表示させる機能を備えた上記USBキーとしているので、コンピュータウィルスに感染したファイルの内容をテキストで確認できる効果がある。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るセキュリティ保全システムの構成ブロック図である。

【図2】ブラウザ及びメーラーの設定変更の処理を示すフロー図である。

【図3】OS状態をチェックして提供する処理を示すフロー図である。

【図4】Webサーバ3における処理を示すフロー図で

16

ある。

【図5】本発明の実施の形態に係る別のセキュリティ保全システムのUSBキー内における起動プログラムの処理の流れを示すフローチャートである。

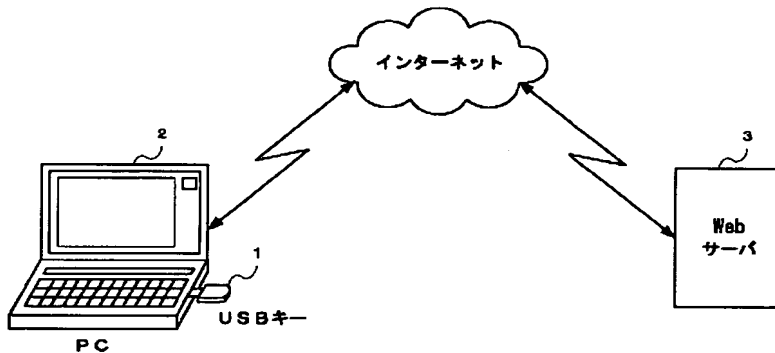
【図6】本発明の別の実施の形態に係るセキュリティ保全システムにおけるサーバでの処理の流れを示すフローチャートである。

【図7】本発明の実施の形態に係るセキュリティ設定の画面の概略図である。

10 【符号の説明】

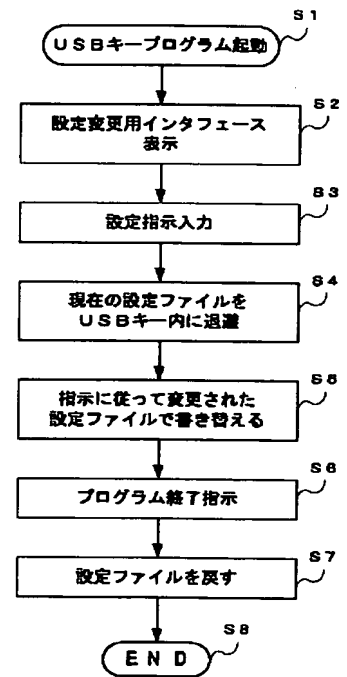
1…USBキー、 2…PC、 3…Webサーバ

【図1】



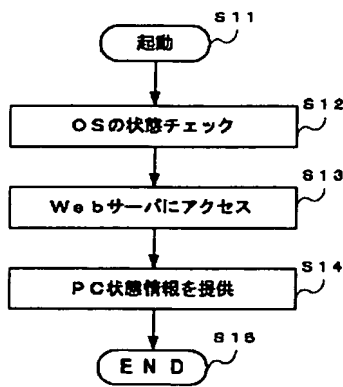
【図1】

【図2】



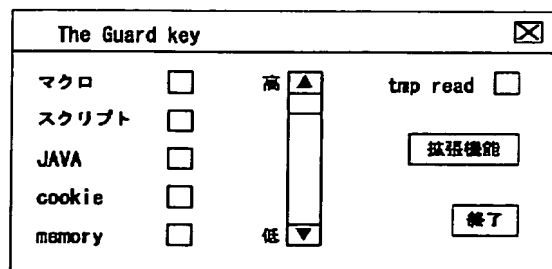
【図2】

【図3】



【図3】

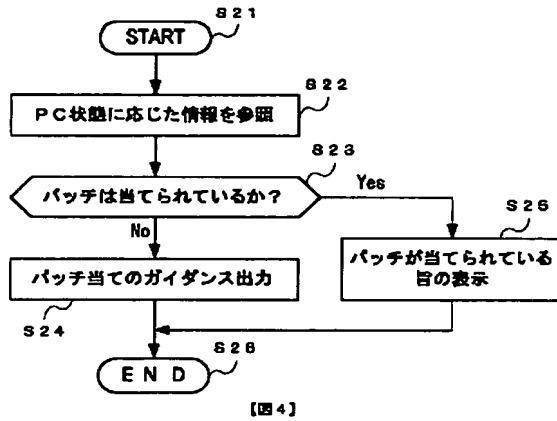
【図7】



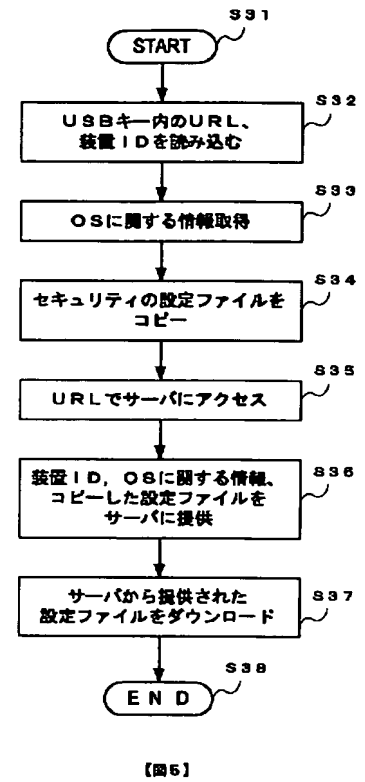
【図7】

(10)

【図4】

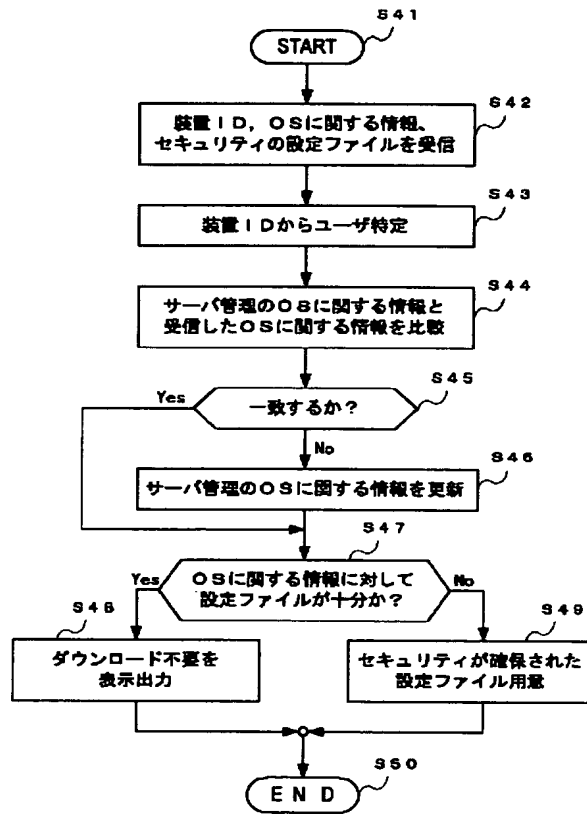


【図5】



(11)

【図 6】



【図 6】